

Application No. 09/863,301

Reply to Official Action mailed on March 09, 2005

### **Remarks/Arguments**

Claims 1-20 remain in the case. Claims 1,2, 4-6 and 11-13 have been amended. Claims 3, 7-10, and 14-20 remain in their original form. No claims have been withdrawn.

Claims 1,2, 4-6 and 11-13 have been amended to avoid invoking 35 U.S.C. 112, sixth paragraph. In particular, all instances of phrases such as —the step of— have been deleted. Applicant wishes to note for the record that the amendments are neither narrowing, nor are the amendments being made for a reason substantially related to patentability. Applicant respectfully submits that no new matter has been added in the amendments.

Independent claim 4 has been amended to correct a clerical error. Specifically, “toring” has been changed to “storing”.

### **Claim Rejections Under 35 USC § 102**

*Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,219,793 by Li et al. (Li).*

The cited reference of Li describes a system in which a mobile telephone (ref Li, Fig. 1, item 102) comprises a fingerprint scanner. When a user goes to use the phone, a biometric input is received. In Li, data associated with the biometric input is transmitted to a remote mobile switching center (ref Li, Fig. 1, item 103). The mobile switching center compares the data associated with the biometric input against data in a “challenge key database” (ref Li, Fig. 1, item 107). When the data comparison is indicative of a match the user of the mobile phone is authorized to use the phone normally. The cited reference of Li also teaches that an owner of the mobile phone of Li serves as a “master user” (ref. Li, col 15, lines 15 to 30.) Li teaches that the master user authorized other user to use the mobile phone by authenticating the master user and then authenticating the additional user (or users) and having data according to their biometric information stored on the remote mobile switching center.

*Application No. 09/863,301*

*Reply to Official Action mailed on March 09, 2005*

Independent claim 1 has been amended to clearly differentiate it from the cited reference of Li. Amended independent claim 1 clearly states,

*"...if the comparison result is indicative of a match:*

*providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service for a predetermined, said access provided for a predetermined, limited period of time."*

In the cited reference of Li, there is no mention of a duration in which an additional user is authorized. Thus, in the cited reference of Li unless the master user makes the effort of changing the authorization status of an additional user, the additional user will be able to use the mobile phone of Li. Amended independent claim 1 clearly states, "...enabling wireless signals provided by the third party to access the secure entity or service, said access provided for a predetermined, limited period of time." Li does not teach this. Specifically, Li makes no mention of providing access for a limited period of time. Therefore, the cited reference of Li does not anticipate amended independent claim 1. Similarly, a person of ordinary skill in the art having reviewed and understood Li would not be lead to provide a system according amended independent claim 1. Therefore, amended independent claim 1 is not obvious in light of Li in isolation.

### **Claim Rejections Under 35 USC § 103**

*Claims 2-20 are rejected under 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office Action. Specifically, claims 2-20 are rejected as being obvious in light of the combination of Li and US patent 5,969,632 by Diamant et al. (Diamant).*

As explained in the arguments regarding anticipation of amended independent claim 1 in light of Li, Li does not render amended independent claim 1 obvious. Specifically, Li does not teach or suggest providing gated access to a third party for a predetermined, limited period of time. The cited reference of Diamant does not teach providing gated access to a third party for a predetermined, limited period of time. As

Application No. 09/863,301

Reply to Official Action mailed on March 09, 2005

neither of these cited references teach this limitation it is apparent that amended independent claim 1 is not obvious in light of Li in combination with Diamant.

Claim 2 depends from amended independent claim 1. Since claim 1 is not obvious in light of the combination of Li and Diamant, it is clear that claim 2 cannot be obvious in light of the same combination of cited references.

Regarding claim 3 Examiner stated, "Diamant further teaches: 1) wherein the flag state after a predetermined amount of time [ie. referring to fig. 8, steps 500 and 506 disclose the device sets a security flag to on and off (col.13, lines 21-42)]" Having carefully reviewed the Fig. 8 and the cited text of Diamant Applicant was unable to find any reference to time or a similar notion of a limited duration during which access is granted to a third party. Therefore, Applicant is unable to fully appreciate the justification for the obviousness rejection stated by Examiner. Applicant is unable to find any reference in Diamant relating to setting a flag for a limited period of time and therefore, Applicant respectfully asserts that a limitation taught in claim 3 is not present in Diamant. Similarly, Applicant asserts that said Li does not teach this limitation and therefore claim 3 is not obvious in light of the combination of Li and Diamant. Additionally, claim 3 depends from amended independent claim 1 which is not obvious in light of Li in combination with Diamant and, therefore, claim 3 cannot be obvious in light of Li in combination with Diamant.

Independent claim 4 has been rejected as being obvious in light of the combination of Li and Diamant. Independent claim 4 states,

*"...if the comparison result is indicative of a match:*

*providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service;*

*receiving the gating signal at the secure entity or service; and,*

*in response to the wireless gating signal, setting a flag within the secure entity or service, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the secure entity or service is non responsive to the wireless signals and in a second other state the secure entity or service is*

Application No. 09/863,3011

Reply to Official Action mailed on March 09, 2005

*responsive to the wireless signals provided by the third party, the flag supporting a timing function such that the flag once set to the second other state returns to the first state after a predetermined, limited period of time absent additional comparison results indicative of a match."*

The cited reference of Li teaches enabling an additional user to use a mobile phone after a biometric data sample from a master user is provided. However, the cited reference of Li does not discuss the notion of supporting access by the additional user for a limited period time. Specifically Li teaches that unless the master user completes a procedure to remove the additional user as an authorized additional user (ref. Li, col. 15 lines 15 to 30) the additional user maintains their ability to use the mobile phone. Thus, it is clear that the method recited in amended independent claim 4 is not obvious in light of Li in isolation.

The cited reference of Diamant does not teach providing gated access to secure content for a predetermined, limited period of time. Therefore amended independent claim 4 is not obvious in light of Diamant isolation. As neither Li nor Diamant teach or suggest the notion of providing gated access to a third party for a predetermined limited period of time it is unclear how a person of ordinary skill in the art would combine them to provide a method according to amended independent claim 4. Therefore, amended independent claim 4 is not obvious in light of the combination of Li and Diamant.

Claims 5-7 depend from amended independent claim 4. Since amended independent claim 4 is not obvious in light of the combination of Li and Diamant it is clear that claims 5-7 cannot be obvious in light of the same combination of cited references.

Claim 8 states, "...wherein different persons of the plurality of persons have different predetermined access privileges." Applicant asserts that Li does not teach this. Specifically, Li teaches that master user permits additional users to use a mobile phone however Li does not suggest that the access privileges of the additional users are different from each other, only that they are different from the access privileges of the master user. The cited reference of Diamant does not teach the notion of providing gated access to third parties in which the third parties "have different predetermined access privileges" as

Application No. 09/863,3011

Reply to Official Action mailed on March 09, 2005

recited in claim 8. Thus, clearly neither Li nor Diamant teach the limitation of claim 8 and therefore it is not apparent how a person of ordinary skill in the art would arrive at such a method having reviewed and understood the teachings of Li and Diamant. Further, claim 8 depends from amended independent claim 4, which is not obvious in light of Li in combination with Diamant. Therefore, claim 8 cannot be obvious in light of Li in combination with Diamant.

Claims 9 and 10 depend from claims 4 and 8, which are not obvious in light of the combination of Li and Diamant. Therefore, claims 9 and 10 cannot be obvious in light of Li in combination with Diamant

Independent claim 11 has been rejected as being obvious in light of the combination of Li and Diamant. Claim 11 states,

*"A method for providing gated access for a third party to a secure entity or service comprising :*

*providing to a first designated user other than the third party a first portable biometric device operable to capture biometric information presented thereto, the portable biometric device having stored biometric data in dependence upon a biometric characteristic of the first designated user;*

*providing the third party with a second other portable biometric device operable to capture biometric information presented thereto, the second portable biometric device having stored biometric data in dependence upon a biometric characteristic of the third party;*

*capturing biometric information representative of a biometric characteristic in response to the first designated user presenting said information to the first portable biometric device and providing biometric data in dependence thereupon;*

*comparing the captured biometric data with the stored biometric data in the first portable biometric device to produce a comparison result; and,*

*if the comparison result is indicative of a match, performing:*

Application No. 09/863,3011

Reply to Official Action mailed on March 09, 2005

*providing a wireless gating signal from the first portable biometric device for enabling wireless signals provided by the third party to access the secure entity or service;*

*receiving the gating signal at a port of the secure entity or service; and, in response to the wireless gating signal, setting a flag within a locking mechanism of the secure entity or service, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the locking mechanism is non responsive to the wireless signals and in a second other state the locking mechanism is responsive to the wireless signals provided by the third party."*

The cited reference of Li teaches that (ref. Li, col 15 beginning line 16), "...multiple users can be permitted to use the same wireless phone. All that is required is that MCKD 107 at the CAS 106 be allowed to contain multiple CKs 202, one generated from each user of the same phone." Independent claim 11 clearly recites that the first designated user is not the third party and that the first designated user and the third party each have access to a different "portable biometric device." Li does not teach or suggest that the first designated user, ie the "master user" of Li, and the third party, ie. the "additional user" of Li, have their own separate portable biometric device. Instead, Li is focused on the use of a same one device. A person of skill in the art having reviewed and understood Li would not think to provide separate portable biometric devices to the first designated user and the third party. Therefore, claim 11 is not obvious in light of Li.

The cited reference of Diamant does not teach providing portable biometric devices. Therefore, providing separate portable biometric devices to the first designated user and the third party would be outside the scope of Diamant and thereby not obvious in light of Diamant. Since neither Li nor Diamant teach providing separate portable biometric devices to the first designated user and the third party, it is apparent that independent claim 11 is not obvious in light of the combination of Li and Diamant. Claims 12 to 14 depend from independent claim 11. Since independent claim 11 is not obvious in light of the combination of Li and Diamant it is clear that claims 12 to 14 cannot be obvious in light of these cited references.

Application No. 09/863,3011

Reply to Official Action mailed on March 09, 2005

Claims 12 and 13 depend from independent claim 11. Since independent claim 11 is not obvious in light of the combination of Li and Diamant it is apparent that claims 12 and 13 cannot be obvious in light of the combination of Li and Diamant.

Claim 14 recites, "...wherein the wireless gating signal from the first portable biometric device and the wireless signal from the second portable biometric device are received at different ports of the secure entity or service." A person of ordinary skill in the art having reviewed and understood Li would likely assume that the mobile phone would use the same infrastructure regardless of whether the user of the mobile phone is the "master user" or an "additional user." As such it would not be obvious to that person to support wireless gating signals wherein, "the wireless gating signal from the first portable biometric device and the wireless signal from the second portable biometric device are received at different ports of the secure entity or service", as recited in claim 14.

Therefore, it is apparent that the cited reference of Li, in isolation, does not render claim 14 obvious. As the cited reference of Diamant does not specifically address gated access via wireless networks, but instead addresses data transfer within a network infrastructure it is apparent that Diamant, in isolation, does not render the method of claim 14 obvious. As neither Diamant nor Li teach the limitations of claim 14 as described above, it is clear that a person of ordinary skill in the art would not be lead to the method of claim 14 by the combination of Li and Diamant. Further, claim 14 depends from independent claim 11. As independent claim 11 is not obvious in light of Li in combination with Diamant, it is clear that claim 14 cannot be obvious in light of Li in combination with Diamant.

Independent claim 15 has been rejected as being obvious in light of the combination of Li and Diamant. Independent claim 15 states,

*"A security system for securing an entity or a service from indiscriminate access and for providing gated access for a third party, the security system comprising:*

*at least a portable biometric device, the device comprising:*

*a biometric sensor for capturing biometric information representative of a biometric characteristic in response to a person presenting said information to the portable biometric device;*

Application No. 09/863,3011

Reply to Official Action mailed on March 09, 2005

*an encoder for digitally encoding the captured biometric information and providing biometric data in dependence thereupon;*

*memory for storing biometric data indicative of a biometric characteristic of a first designated user;*

*a processor for comparing the captured biometric data with stored biometric data to produce a comparison result, and if the comparison result is indicative of the first designated user for providing a wireless gating signal for enabling wireless signals provided by the third party to access the secure entity or service, and if the comparison result is indicative of the third party for providing a wireless signal; and,*

*a transmitter for wireless transmission of the wireless gating signal or the wireless signal;*

*at least a port for receiving the wireless gating signal and the wireless signal from the portable biometric device; and,*

*a locking mechanism for securing the entity or service, the locking mechanism comprising a processor for setting a flag in response to the wireless gating signal, the flag for use in gating received wireless signals for controlling access to the secure entity or service such that in a first state the locking mechanism is non responsive to the wireless signals and in a second other state the locking mechanism is responsive to the wireless signals provided by the third party."*

The cited reference of Li provides a system in which a user authenticates by providing a biometric input. Data relating to the biometric input is provided to a remote server for comparison with other biometric data. If a match is found then the user is authenticated. (Reference Li, Fig. 1 and Abstract) Li does not teach that the authentication process is carried out using a processor and memory that are part of a portable biometric device. Thus, Li, in isolation, does not render the invention as recited in independent claim 15 obvious. The cited reference of Diamant does not teach a portable biometric device either. Therefore, it would not be apparent to combine the cited references of Li and Diamant to provide a portable biometric device supporting biometric authentication and for matching biometric data on the portable biometric device according to independent claim 15 and, therefore, claim 15 is not obvious in light of the combination of Li and Diamant.

*Application No. 09/863,3011*

*Reply to Official Action mailed on March 09, 2005*

Claim 17 states, "... wherein the security system comprises a first portable biometric device for use by the first designated user and a second other portable biometric device for use by the third party." The cited reference of Li teaches that same device is useable by a third party once it has been enabled for their use by a master user (ref. Li, col. 15 lines 15 to 30.) The cited reference of Diamant teaches a security system for a network having private and public portions. Diamant does not teach or suggest a method consistent with the method of claim 17. Thus, clearly, claim 17 is not obvious in light of the combination of Li and Diamant.

Claims 16 to 20 depend from independent claim 15. Since independent claim 15 is not obvious in light of Li in combination of Diamant claims 16 to 20 cannot be obvious in light the cited references.

Applicant looks forward to favourable reconsideration of the present application.

No new matter has been added.

**Please charge any additional fees required or credit any overpayment to Deposit Account No: 50-1142.**

Respectfully submitted,



Gordon Freedman, Reg. No. 41,553

Freedman and Associates  
117 Centrepointhe Drive, Suite 350  
Nepean, Ontario  
K2G 5X3 Canada

Tel: (613) 274-7272  
Fax: (613) 274-7414  
Email: [Gordon@freedmanandassociates.ca](mailto:Gordon@freedmanandassociates.ca)  
GF/VL/bh